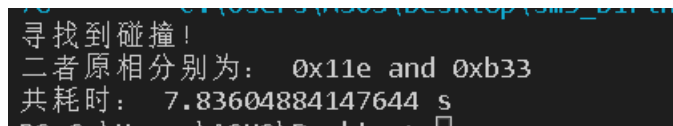


Project: implement the naïve birthday attack of reduced SM3

代码说明：首先按照 sm3 算法把 sm3 的代码写出来，然后利用生日攻击构造碰撞：由于 sm3 输出为 256 位比特，如果需要构造完全的碰撞则大约需要 $1.177\sqrt{2^n}$ 个值，较大，故我们从实验的角度，构造前 6 位碰撞，具体思路为输入大量随机数进入 sm3 函数，比较所有输出的前 6 位，发现相同的即碰撞完成。

运行指导：直接运行 py 文件

运行结果截图：



```
7.83604884147644 s
寻找碰撞！
二者原相分别为： 0x11e and 0xb33
共耗时： 7.83604884147644 s
```